UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
WHITE PLAINS DIVISION

Lavina Henderson and Jeremy Henderson, Individually and on behalf of all others similarly situated, **Plaintiffs,** **v.** **Somnia, Inc. and Resource Anesthesiology Associates of NM Inc.,** **Defendants.**	Case No. _____ Judge _____ JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Lavina and Jeremy Henderson (collectively, "Plaintiffs") bring this Class Action Complaint against Somnia, Inc. ("Somnia") and Resource Anesthesiology Associates of NM Inc. (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

BACKGROUND

1. Plaintiffs seek recovery, on behalf of themselves and those similarly situated, with respect to the data security incident that, upon information and belief, occurred in Defendant Somnia's security network and affected over 410,000 individuals nationwide.[1]

[1] https://www.hipaajournal.com/data-breach-impacts-more-than-one-dozen-anesthesia-providers/ (last visited: November 4, 2022).

2. Defendant Somnia is "a practice management company singularly focused on anesthesiology.[2]

3. As part of its services, Defendant Somnia provides record-keeping and management services for anesthesia medical practices across the country. This includes storing and maintaining patients' names, addresses, health insurance policy numbers, payment information, Social Security numbers, and diagnosis and treatment information[3] ("Private Information").

4. Upon information and belief, on or around July 11, 2022, Defendant Somnia identified suspicious activity on its system and found that Plaintiffs' and Class Members' Private Information may have been compromised (the "Data Breach").[4]

5. As a result of the Data Breach, it is believed that Defendant Somnia's inadequate security measures led to the disclosure of the following information: names, addresses, health insurance policy numbers, payment information, Social Security numbers, and diagnosis and treatment information for at least 410,000 individuals.[5]

6. Upon information and belief, Defendant Somnia is Defendant Resource Anesthesiology Associates of NM Inc.'s management company.

7. Plaintiffs sought medical treatment at Defendant Resource Anesthesiology Associates of NM Inc.

8. Defendant Resource Anesthesiology Associates of NM Inc. is a healthcare provider in New Mexico that, upon information and belief, provides anesthesia-related medical services.[6]

---

[2] See https://somniaanesthesiaservices.com/somnia-anesthesia (last viewed: November 21, 2022).
[3] *Supra* Fn. 1.
[4] *Id*.
[5] *Id*.
[6] https://opennpi.com/provider/1386929644 (last viewed: November 4, 2022).

9. As a condition of receiving medical treatment at its medical centers, Defendant Resource Anesthesiology Associates of NM Inc. required Plaintiff Lavina Henderson to provide her name, Social Security number, and some combination of the following elements: date of birth, driver's license number, financial account information, health insurance policy number, medical record number, Medicaid or Medicare ID, and health information such as treatment and diagnosis information (collectively, "Protected Health Information" or "PHI").

10. As a condition Defendant Resource Anesthesiology Associates of NM Inc. required Plaintiff David Henderson to provide his name, and some combination of the following elements: date of birth, driver's license number, financial account information, health insurance policy number, medical record number, Medicaid or Medicare ID, and health information such as treatment and diagnosis information (collectively, "Protected Health Information" or "PHI").

11. In order to provide medical services, Defendants Resource Anesthesiology Associates of NM Inc. used Defendant Somnia to provide administrative services, including the storage of Plaintiffs' and Class Members' protected health information.

12. Upon information and belief, Defendant Resource Anesthesiology Associates of NM Inc. entrusted Defendant Somnia with Plaintiffs' and Class Members' PHI.

13. Plaintiffs Lavina Henderson received a letter titled "Notice of Data Security Incident" on or around October 24, 2022 ("Notice of Data Security Incident Letter").

14. Plaintiffs David Henderson also received a Notice of Data Security Incident Letter on or around October 24, 2022.

15. Plaintiffs Lavina Henderson's Notice of Data Security Incident Letter stated the following:

What Happened?

On July 11, 2022, Resource Anesthesiology Associates of NM Inc.'s management company identified suspicious activity on its systems. The management company immediately implemented its incident response protocols, disconnected all systems, and engaged external cybersecurity experts to conduct a forensic investigation. The investigation stored on the management company's systems may have been compromised. The management company then reviewed the potentially impacted information to identify any protected health information that may have been affected. This review was recently completed, at which point we determined that your protected health information may have been affected.

What Information was Involved?
Impacted information may include your name, Social Security Number, and some combination of the following elements: date of birth, driver's license number, financial account information, health insurance policy number, medical record number, Medicaid or Medicare ID, and health information such as treatment and diagnosis information.

16. Notably, the Notice of Data Security Incident Letter sent to Plaintiffs in this case mirrors the Notice of Data Security Incident Letter sent to patients in the Anesthesia Associates of El Paso Data Breach.[7]

17. Upon information and belief, Plaintiffs' Private information was disclosed in the Data Breach that occurred in Defendant Somnia's network. In turn, as described below, Plaintiffs were substantially harmed as a result of Defendant Somnia's Data Breach.

18. Upon information and belief, the Data Breach at Defendant Somnia extends to over 16 anesthesia medical practices across the country, totaling in excess of 410,832 individuals.[8]

Name of Covered Entity	Individuals Affected
Providence WA Anesthesia Services PC	98,643
Palm Springs Anesthesia Services PC	58,513
Anesthesia Services of San Joaquin PC	44,015
Anesthesia Associates of El Paso PA	43,168
Resource Anesthesiology Associates PC	37,697

[7] *Compare* ¶ 13 *with* https://ago.vermont.gov/blog/2022/10/24/anesthesia-associates-of-el-paso-data-breach-notice-to-consumers/?utm_source=rss&utm_medium=rss&utm_campaign=anesthesia-associates-of-el-paso-data-breach-notice-to-consumers (last visited: November 4, 2022).
[8] https://www.hipaajournal.com/data-breach-impacts-more-than-one-dozen-anesthesia-providers/ (last visited: November 4, 2022).

Resource Anesthesiology Associates of IL PC	18,321
Bronx Anesthesia Services PC	17,802
Resource Anesthesiology Associates of CA A Medical Corporation	16,001
Hazleton Anesthesia Services PC	13,607
Anesthesia Associates of Maryland LLC	12,403
Somnia Pain Mgt of Kentucky	10,849
Upstate Anesthesia Services PC	9,065
Resource Anesthesiology Associates of KY PSC	8,995
Saddlebrook Anesthesia Services PC	8,861
Fredericksburg Anesthesia Services LLC	7,069
Lynbrook Anesthesia Services PC	3,800
Somnia, Inc.	1,326
Mid-Westchester Anesthesia Services	707
Total	**410,842**

19. In other words, the data breach that affected patients at Defendant Resource Anesthesiology Associates of NM Inc. is part of the Data Breach at Defendant Somnia, which has affected over 410,000 Class Members across the country.

20. Plaintiffs and Class Members are individuals whose PHI was acquired, stored, and utilized by Defendants for its business and financial benefit.

21. By obtaining, collecting, utilizing, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations to keep Plaintiffs' and Class Members' Private Information confidential, safe, secure, and protected from the unauthorized access, disclosure, and theft in foreseeable data breach incidents.

22. Defendants, however, disregarded their duties and obligations and the privacy rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable data security measures to protect and

safeguard the Private Information of Plaintiffs and Class Members, by allowing the Private Information to be stored and maintained in a vulnerable state.

23. Defendant Resource Anesthesiology Associates of NM Inc. admitted on its Notice of Data Security Letter to Plaintiffs and the Class Members that the unencrypted Private Information impacted during the Data Breach included Protected Health Information.

24. The exposed Private Information of Plaintiffs and Class Members is highly sensitive and can be utilized to commit identity theft and fraud. The Private Information has been or likely will be sold on the dark web, as this is the *modus operandi* for cyber criminals targeting this type of Private Information. Plaintiffs and Class Members, therefore, are now at a current and ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers—the gold standard for identity thieves.

25. While many details of the Data Breach remain in the exclusive control of Defendants, upon information and belief, Defendants breached its duties and obligations by failing, in one or more of the following ways: (1) to design, implement, and maintain reasonable network safeguards against foreseeable threats; (2) to design, implement, and maintain reasonable data retention policies; (3) to adequately train employees on data security; (4) to comply with industry-standard data security practices; (5) to warn Plaintiffs and Class Members of Defendants' inadequate data security practices; (6) to adequately encrypt the Private Information; (7) to utilize widely available software able to detect and prevent cyberattacks; and (8) otherwise fail to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

26. Moreover, despite learning of the Data Breach in July 2022, Defendant Resource Anesthesiology Associates of NM Inc. did not begin notifying Plaintiffs and Class Members until

early October 2022. Likewise, Defendant Somnia has *still* not notified Plaintiffs and Class Members.

27. As a result of Defendants' acts and omissions, Plaintiffs and Class Members had their most sensitive Private Information stolen by malicious cybercriminals. The information that was compromised is a one-stop shop for identity thieves to wreak havoc on Plaintiffs' and Class Members' personal and financial lives. Given the sensitivity and static nature of the information involved (such as names, Social Security numbers, and dates of birth), the risk of identity theft is present, materialized, and will continue into the foreseeable future for Plaintiffs and Class Members. Plaintiffs and Class Members will therefore now live with the present and ongoing risk of identity theft, which will require third-party professional services to monitor their Private Information for criminal misuse and dark web activity.

28. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered the following actual and imminent injuries: (i) invasion of privacy; (ii) out-of-pocket expenses; (iii) loss of time and productivity incurred mitigating the present risk and imminent threat of identity theft; (iv) actual identity theft and fraud resulting in additional economic and non-economic damages; (v) diminution of value of their Private Information; (vi) anxiety, stress, nuisance, and annoyance; (vii) increased targeted and fraudulent robocalls and phishing email attempts; (viii) the present and continuing risk of identity theft posed by their Private Information being placed in the hands of the ill-intentioned hackers and/or criminals; (ix) the retention of the reasonable value of the Private Information entrusted to Defendants; and (x) the present and continued risk to Private Information, which remains on Defendants' vulnerable network, placing Plaintiffs and Class Members at an ongoing risk of harm.

29. Plaintiffs bring this class action to remedy these harms, on behalf of themselves and all similarly situated persons whose Private Information was compromised in the Data Breach. Plaintiffs and Class Members seek compensatory damages, incidental damages, and consequential damages for the diminution in value of their Private Information, invasion of their privacy, loss of their time, loss of their productivity, out-of-pocket costs, and future costs of necessary identity theft monitoring. Plaintiffs and Class Members also seek injunctive relief including improvements to Defendants' data security system and protocols, deletion of Private Information that is unnecessary for legitimate business purposes, and future annual audits to protect their Private Information against foreseeable future cyber security incidents.

30. Plaintiffs brings this Consolidated Class Action Complaint against Defendants asserting claims for: (1) negligence, (2) negligence *per se*, (3) negligent entrustment, and (4) breach of fiduciary duty.

PARTIES

Plaintiffs Lavina Henderson

31. Plaintiffs Lavina Henderson is a resident and citizen of New Mexico, residing in Farmington, New Mexico.

32. Plaintiffs received a letter dated October 24, 2022, from Defendant Resource Anesthesiology Associates of NM Inc. The letter stated that Plaintiffs' Private Information may have been compromised in the Data Breach.

Plaintiffs Jeremy Henderson

33. Plaintiffs Jeremy Henderson is a resident and citizen of New Mexico, residing in Farmington, New Mexico.

34. Plaintiffs received a letter dated October 24, 2022, from Defendant Resource Anesthesiology Associates of NM Inc. The letter stated that Plaintiffs' PHI may have been compromised in the Data Breach.

Defendant Resource Anesthesiology Associates of NM Inc.

35. Defendant Resource Anesthesiology Associates of NM Inc is a corporation organized under the laws of New Mexico, and its United States headquarters and principal place of business is located at 206 S. Coronado Ave., Espanola, New Mexico.

Defendant Somnia, Inc.

36. Defendant Somnia, Inc. is a corporation organized under the laws of New York with a principal place of business in Harrison, New York..

JURISDICTION AND VENUE

37. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one member of the class, including some Plaintiffs, are citizens of a state different from Defendants.

38. This Court has personal jurisdiction over Defendants because Defendant Somnia Inc.'s principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

39. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant s principal place of business is in this District.

FACTUAL ALLEGATIONS

Defendants Collect Private Information

40. Defendant Resource Anesthesiology Associates of NM Inc. collects Private Information, including Plaintiffs' Private Information, in order to provide medical services.

41. Upon information and belief, Defendant Somnia stores and maintains Private Information and PHI for more than a dozen anesthesia medical practices, including Defendant Resource Anesthesiology Associates of NM Inc., across the country.

42. The types of private information collected and utilized by Defendants includes, but is not limited to, names, addresses, health insurance policy numbers, payment information, Social Security numbers, and diagnosis and treatment information.

The Data Breach

43. On or around July 11, 2022, Defendant Somnia detected suspicious activity on its systems. [9]

44. The subsequent investigation determined that Plaintiffs' and Class Members' Private Information was compromised in the Data Breach.

45. Defendant Resource Anesthesiology Associates of NM Inc. admits in its Notice of Data Security Incident that highly sensitive categories of PHI were exposed in the Data Breach, including in some instances—Social Security numbers.

46. According to the HIPAA Journal, the Data Breach also involved Private Information, such as the following: names, addresses, health insurance policy numbers, payment information, Social Security numbers, and diagnosis and treatment information.

[9] https://www.hipaajournal.com/data-breach-impacts-more-than-one-dozen-anesthesia-providers/ (last visited: November 4, 2022).

The Data Breach Was Foreseeable and Preventable

47. Cyberattacks or Data Breaches like that experienced by Defendants are a well-known threat to companies that maintain PHI. As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

48. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[10]

49. Before the Data Breach, Defendants knew or should have known that the above security measures were necessary for the prevention of a data breach of this nature.

50. Defendants also could have prevented the Data Breach by encrypting the systems and files containing the Private Information of Plaintiffs and Class Members and by destroying Private Information it no longer had a legitimate need for.

51. Additionally, to prevent and detect unauthorized cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures known to be generally effective at mitigating the risk of a cyberattack:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

[10] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[11]

[11] *Id.* at 3–4.

52. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it. . . .

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[12]

53. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential for compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection

[12] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[13]

54. Given that Defendants were storing the Private Information of Plaintiffs and Class Members, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

55. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the unauthorized exposure and exfiltration of the Private Information of Plaintiffs and Class Members.

56. As evidenced by its computer systems in need of security upgrades, as well as inadequate procedures for handling email phishing attacks, viruses, malignant computer code, and hacking attacks, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

57. Defendants' negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendants to protect and secure sensitive data they possess.

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

[13] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

Value of Private Information

59. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

60. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[16] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18]

61. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[19] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data

[14] 17 C.F.R. § 248.201 (2013).
[15] *Id.*
[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 27, 2021).
[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 27, 2021).
[18] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 27, 2021).
[19] *Data Brokers*, Los Angeles Times, Nov. 5, 2019, *available at* https://www.latimes.com/business/story/2019-11-05/column-data-brokers

broker who in turn aggregates the information and provides it to marketers or app developers.[20, 21] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[22]

62. The integrity of PII gives it its value because PII is used to secure loans, open lines of credit, verify identities, and unlock government benefits. When PII is used to commit fraud, these simple everyday necessities become more difficult, if not impossible, due to lowered credit scores and tarnished credit histories from credit fraud and identity theft.[23]

63. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals and is likely already available on the dark web due to its high value for threat actors. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss.

64. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[24]

[20] https://datacoup.com/
[21] https://digi.me/what-is-digime/
[22] *Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[23] https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft
[24] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 27, 2021).

65. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

66. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

67. Based on the foregoing, the Private Information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The Information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change: Social Security number and name.

68. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[26]

[25] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 27, 2021).

[26] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at* https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 23, 2021).

69. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

70. The fraudulent activity resulting from the Data Breach may not come to light for years.

71. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

72. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information, and PHI in particular, on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

73. According to account monitoring company LogDog, medical data, such as PHI, sells for $50 and up on the Dark Web.[27]

74. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[27] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), *available at* https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited July 20, 2021).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

75. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

76. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages, in addition to any fraudulent use of their Private Information.

77. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

78. To date, Defendants have offered Plaintiffs and Class Members only 12 months of single bureau credit monitoring services through Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here. Moreover, Defendants put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services that it offered.

---

[28] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Aug. 23, 2021).

79. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

80. As a condition of providing medical treatment and services, processing medical claims, sending bills, and providing collection services for treatment, Defendants requires that its customers entrust it with Private Information.

81. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

82. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

83. Plaintiffs and the Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendants' Conduct Violates HIPAA

84. Defendants are required to comply with HIPAA.

85. As a health network and provider, Defendant Resource Anesthesiology Associates of NM Inc. is a covered entity by HIPAA.

86. Upon information and belief, Defendant Somnia is a HIPAA Business Associate and is bound by HIPAA regulations and had a duty to safeguard protected health information that it collects.

87. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

88. Defendants' Data Breach resulted from a combination of insufficiencies that indicate Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Defendants' Data Breach that Defendants either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs and Class Members' Private Information.

89. In addition, Defendants' Data Breach could have been prevented if Defendants implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII and PHI when it was no longer necessary and/or had honored its obligations to its customers.

90. Defendants' security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce in violation of 45 CFR 164.306(a)(4);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*; and

k. Retaining information past a recognized purpose and not deleting it.

91. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400–14, also required Defendants to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[29]

[29] Breach Notification Rule, U.S. DEP'T OF HEALTH & HUMAN SERVICES, *available at* hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Oct. 13, 2020).

92. Because Defendants have failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is necessary to ensure Defendants' approach to information security is adequate and appropriate.

93. Defendants still maintain the Private Information of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs' and Class Members' Private Information remain at risk of subsequent Data Breaches.

Defendants Failed to Comply with FTC Guidelines

94. Defendants were also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

95. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[30]

96. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[31] The guidelines note that businesses should protect the personal customer information that they keep; properly

[30] FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 7, 2022).
[31] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 7, 2022).

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

97. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

98. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

99. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

100. Defendants were at all times fully aware of its obligation to protect the PII stored within its systems because of its position as a leading healthcare business affiliate. Defendants was also aware of the significant repercussions that would result from its failure to do so.

[32] FTC, *Start With Security*, *supra*.

Defendants Failed to Comply with Industry Standards

101. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

102. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendants, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

103. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

104. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

105. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

106. Upon information and belief, Defendants failed to comply with one or more of the foregoing industry standards.

Plaintiff Lavina Henderson's Experience

107. Plaintiff Lavina Henderson is a former patient of Defendant Resource Anesthesiology Associates of NM Inc.

108. As a condition of receiving medical services, Plaintiff provided her name, Social Security number, and some combination of the following elements: date of birth, driver's license number, financial account information, health insurance policy number, medical record number, Medicaid or Medicare ID, and health information such as treatment and diagnosis information. Plaintiff trusted that her Private Information would be safeguarded according to internal policies and state and federal law.

109. Upon information and belief, Plaintiff's Private Information was stored on both Defendants' networks during the Data Breach and presently remains in both Defendants' possession.

110. On approximately October 24, 2022, Defendant Resource Anesthesiology Associates of NM Inc. notified Plaintiff that its management company's network had a Data Breach and her Private Information may have been compromised in the Data Breach. It is believed that Defendant Resource Anesthesiology Associates of NM Inc.'s management company is Defendant Somnia.

111. Defendant Somnia is partly or wholly responsible for the unauthorized disclosure of Plaintiff's Private Information.

112. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or

any other unsecured source. Plaintiff stores any documents containing her Private Information in a safe and secure location or destroys the documents.

113. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the Notice of Data Security Incident, exploring credit monitoring and identity theft protection services, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

114. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

115. Plaintiff has suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

116. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendants' delay in revealing the true nature of the threat to Plaintiffs' Private Information.

117. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from future breaches**.**

Plaintiffs Jeremy Henderson's Experiences

118. Plaintiff Jeremy Henderson is a former patient of Defendant Resource Anesthesiology Associates of NM Inc.

119. As a condition of receiving medical services, Plaintiff provided his name, driver's license number, financial account information, health insurance information, health insurance policy number, medical record number, Medicaid or Medicare ID, and health information such as treatment and diagnosis information. Plaintiff trusted that his Private Information would be safeguarded according to internal policies and state and federal law.

120. Upon information and belief, Plaintiff's Private Information was stored on both Defendants' networks during the Data Breach and presently remains in both Defendants' possession.

121. On approximately October 24, 2022, Defendant Resource Anesthesiology Associates of NM Inc. notified Plaintiff that its management company's network had a Data Breach and his PHI may have been compromised in the Data Breach.

122. It is believed that Defendant Resource Anesthesiology Associates of NM Inc.'s management company is Defendant Somnia.

123. Defendant Somnia is partly or wholly responsible for the unauthorized disclosure of Plaintiff's Private Information.

124. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing his Private Information in a safe and secure location or destroys the documents.

125. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the Notice of Data Security Incident, exploring credit monitoring and identity theft protection services, and

self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

126. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiffs entrusted to Defendants, which was compromised in and as a result of the Data Breach.

127. Plaintiff has suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

128. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendants' delay in revealing the true nature of the threat to Plaintiffs' Private Information.

129. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from future breaches

Common Injuries & Damages to Plaintiffs and Class Members

130. As result of Defendants' ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

131. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d)

"out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

132. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

133. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

134. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[33] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[34] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

135. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII and PHI at issue here.[35] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[36]

136. As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[37]

---

[33] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/
[34] *Id.*
[35] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web
[36] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/
[37] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web

137. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[38] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[39]

138. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

139. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

[38] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/
[39] *Id.*

140. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[40]

141. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendants did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.[41]

142. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

143. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

144. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiffs and Class Members will need to be remain vigilant against unauthorized data use for years or even decades to come.

145. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner

[40] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed October 21, 2022).
[41] *Id.*

Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[42]

146. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[43]

147. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[44]

148. Defendants' failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability

[42] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited May 28, 2015).
[43] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[44] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last accessed: October 21, 2022).

to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

149. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

150. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

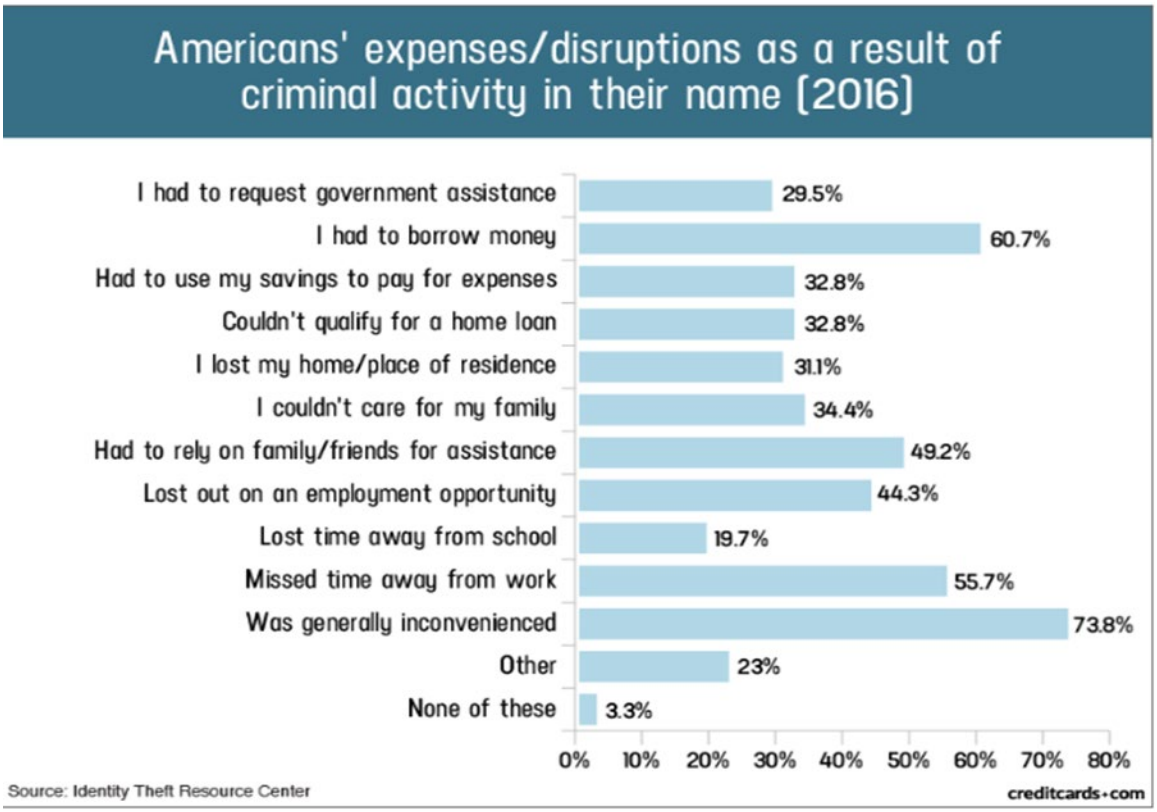
151. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[45]

152. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider

[45] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[46]

153. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[47]



154. PII/PHI is a valuable property right.[48] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison

[46] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[47] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).
[48] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

155. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

156. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[49]

157. To date, Defendants have done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach -- Defendant Resource Anesthesiology Associates Of NM, Inc. has only offered 12 months of inadequate identity monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the foreseeable future.

158. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. Defendant Resource Anesthesiology Associates Of NM, Inc also places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

[49] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

159. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, reports of misuse of Class Member PII discussed below, and reports of dissemination on the Dark Web also discussed below, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims

160. It must be noted there may be a substantial time lag—measured in years— between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

161. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

162. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

breach, where victims can easily cancel or close credit and debit card accounts.[50] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

163. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

164. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendants' failure to safeguard their Private Information.

165. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendants for the services, under certain terms, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

166. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not

[50] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

CLASS ALLEGATIONS

167. Plaintiffs brings this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

168. The Nationwide Class that Plaintiffs seeks to represent is defined as follows:

> **All United States residents whose Private Information was actually or potentially accessed or acquired during the Data Breach that took place on or around July 11, 2022 (the "Nationwide Class")**

169. Plaintiffs also seeks to represent the following subclass:

> **All United States residents whose Private Information was actually or potentially accessed or acquired during the Data Breach that took place on or around July 11, 2022, as a result of Defendant Resource Anesthesiology Associates of NM Inc.'s negligent entrustment of data security to Defendant Somnia, Inc. (the "Negligent Entrustment Sub-Class")**

170. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

171. Plaintiffs reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

172. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are no less than 410,000, if not millions, of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendants' records.

173. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Defendants violated the consumer protection statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, incidental, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

174. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach due to Defendants' misfeasance.

175. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to an individual Plaintiffs.

176. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seeks no relief that is antagonistic or adverse to the Members of the Class, and the infringement of the rights and the damages Plaintiffs has suffered are typical of other Class Members. Plaintiffs has also retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously.

177. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

178. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered;

proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

179. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

180. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

181. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

182. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

183. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

CAUSES OF ACTION[51]

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

184. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

185. Plaintiffs and Class Members entrusted Defendants with their Private Information.

186. Plaintiffs and Class Members entrusted their Private Information to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

187. Defendants have and have had full knowledge of the sensitivity of the Private Information and PHI and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

188. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

189. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the Private Information of Plaintiffs and the Class in Defendants' possession was adequately secured and protected.

[51] Hereinafter, the term "Defendants" applies to Defendant Resource Anesthesia Of NM, Inc. and Defendant Somnia, Inc. separately and/or jointly.

190. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain pursuant to regulations.

191. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Class.

192. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential Private Information, a necessary part of obtaining services from Defendants. That duty further arose because Defendants chose to collect and maintain Plaintiffs' and Class Members' Private Information for its own pecuniary benefit.

193. Defendants was subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

194. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

195. Plaintiffs and the Class Members' injuries were the foreseeable and probable result of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

196. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included

their decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiffs and the Class, including basic encryption techniques freely available to Defendants.

197. Plaintiffs and Class Members had no ability to protect their Private Information that was within, and on information and belief remains within, Defendants' possession.

198. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

199. Defendants had (and continues to have) a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

200. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs sand the Class.

201. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

202. Defendants, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and the Class during the time the Private Information was within Defendants' possession or control.

203. Defendants improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

204. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiffs and the Class in the face of increased risk of theft.

205. Defendants, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

206. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the Private Information of Plaintiffs and the Class would not have been compromised.

207. There is a close causal connection between Defendants' failure to implement adequate data security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

208. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to decide how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect,

contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

209. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

210. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants continue to fail to undertake appropriate and adequate data security measures to protect the Private Information in its continued possession.

211. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class)

212. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

213. Plaintiffs and the Class repeat and re-allege each and every allegation in the Petition as if fully set forth herein.

214. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

215. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

216. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

217. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

218. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and by not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

219. Defendants' violation of Section 5 of the FTC Act is, in and of itself, evidence of Defendants' negligent data security practices and further constitutes negligence *per se*.

220. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

221. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

222. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

223. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

224. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet its duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information. Defendants, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

225. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the Private Information of Plaintiffs and the Class would not have been compromised.

226. There is a close causal connection between Defendants' failure to implement adequate data security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

227. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

228. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

229. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private

Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants continue to fail to undertake appropriate and adequate data security measures to protect the Private Information in its continued possession.

230. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class Members are entitled to recover actual, consequential, and nominal damages.

231. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

232. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
NEGLIGENT ENTRUSTMENT [52]
(On Behalf of Plaintiffs and the Negligent Entrustment Class)

233. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

234. Plaintiffs and Class Members entrusted Defendant Resource Anesthesiology Associates Of NM Inc. with their Private Information and PHI.

235. By accepting Plaintiffs' and Class Members' Private Information and PHI, Defendant Resource Anesthesiology Associates Of NM Inc. had a duty to protect and safeguard this information.

[52] In the alternative of their negligence claims, Plaintiffs plead Defendant Resource Anesthesiology Associates Of NM Inc. negligently entrusted Plaintiffs' and Class Members' Private Information to Defendant Somnia.

236. This duty extended to Plaintiffs' and Class Members' Private Information and PII even if Defendant Resource Anesthesiology Associates Of NM Inc. utilized third-party vendors, like Somnia, Inc., to store and safeguard this information.

237. Said differently, if used a vendor to store and protect Plaintiffs' and Class Members' Private Information and PHI, Defendant Resource Anesthesiology Associates Of NM Inc. had a duty to ensure the vendor used reasonable safeguards to protect this information.

238. Defendant Resource Anesthesiology Associates Of NM Inc. breached its duty to entrust Plaintiffs' and Class Members' Private Information and PHI by entrusting this information to a negligent management company.

239. Defendant Resource Anesthesiology Associates Of NM Inc. did not properly vet Defendant Somnia as a management company to store and safeguard Plaintiffs' and Class Members' Private Information and PHI.

240. As a direct and proximate result of Defendant Resource Anesthesiology Associates Of NM Inc.'s negligent entrustment of Private Information and PHI, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

241. As a direct and proximate result of Defendant Resource Anesthesiology Associates Of NM Inc.'s negligent entrustment of Private Information and PHI, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

242. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

243. Plaintiffs and Class Members conferred a monetary benefit on Defendants by providing Defendants, directly or indirectly, with their valuable Private Information.

244. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

245. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

246. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

247. Defendants acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

248. If Plaintiffs and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

249. Plaintiffs and Class Members have no adequate remedy at law.

250. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

251. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

252. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

COUNT V
DECLARATORY RELIEF
(On behalf of Plaintiff and the Nationwide Class)

253. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

254. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

255. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, as well as whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

256. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

257. Defendant still possesses the Private Information of Plaintiff and the Class.

258. To Plaintiff's knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

259. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

260. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial.

261. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Convergent, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

262. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Convergent, thus eliminating the additional injuries that would result to Plaintiff and Class Members.

263. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner; and

e. conducting regular database scans and security checks; and routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiffs and their Counsel to represent the Classes;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and

assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: November 22, 2022

Respectfully Submitted,

/s/ Victoria Maniatis

Victoria Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (212) 594-5300
vmaniatis@milberg.com

Gary M. Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

David K. Lietz (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave. NW, Suite 440
Washington, D.C. 20015
Telephone: (866) 252-0878
dlietz@milberg.com

Counsel for Plaintiffs and Putative Class